APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/593,677	06/14/2000	Noboru Katta	NAK1-BL38	7941

21611   7590   02/11/2004

SNELL & WILMER LLP
1920 MAIN STREET
SUITE 1200
IRVINE, CA 92614-7230

EXAMINER
SIMITOSKI, MICHAEL J

ART UNIT	PAPER NUMBER
2134	4

DATE MAILED: 02/11/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/593,677	KATTA ET AL.
	Examiner	**Art Unit**	
	Michael J Simitoski	2134	

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 June 2000*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-84* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5,7-14,16-27,29-31,33,34,36-39,41-44,46-48,50-63,65-79 and 81-84* is/are rejected.

7)☒ Claim(s) *6,15,28,32,35,40,45,49,64 and 80* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 June 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☒ All b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

   a)☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *3* .

4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: .

DETAILED ACTION

1.   The IDS of 10/06/2000 was received and considered.

2.   Claims 1-84 are pending.

Claim Rejections - 35 USC § 112

3.   The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4.   Claims 7, 33, 36, 38, 46 & 77 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

     a.   Regarding claims 7, 36, 46 & 77, it is unclear how bit data, which is detected by a "detect instruction" can affect the "order in which the ... detect instructions are performed".

     b.   Regarding claim 33, the claim recites "the bit sequence" in both lines 4 and 5, but bit sequence is associated with a "sync pattern" (see claim 31) and "flag pattern" (see claim 33) and is therefore unclear as to which "bit sequence" claim 33 is referring to.

     c.   Regarding claim 38, the claim is indefinite because the claim is incomplete: "the cryptographic processing means ... using the specified". *For the purposes of this office action, line 7 of claim 38 is understood to read "specified algorithm".*

Claim Rejections - 35 USC § 102

5.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6.   Claims 42-44, 47, 48, 66-69 & 84 are rejected under 35 U.S.C. 102(b) as being

anticipated by U.S. Patent 5,548,648 to Yorke-Smith.

Regarding claim 42, Yorke-Smith discloses a content data obtaining means/input means

for obtaining content data (see Fig. 7), a cryptographic information obtaining means/input means

for obtaining cryptographic information/control block including information specifying a part on

which cryptographic processing/decryption is to be performed in the contents data/data segment

(see col. 2, lines 65-67 & col. 3, lines 1-9), the information including a reference instruction/(S

and L_2) indicating that the data section/segment in the content data be referred to (see col. 5,

lines 23-37), a part specifying means for specifying the certain part of the content data based on

the cryptographic information (see col. 3, lines 1-9 & col. 4, lines 23-54), by referring to the data

section/segment as indicated by the reference instruction/(S and L_2) (see col. 5, lines 23-37 &

col. 9, lines 15-26), and a cryptographic processing means for performing one of encryption and

decryption on the certain part (see Fig. 6 & Fig. 7).

Regarding claim 43, Yorke-Smith discloses that the cryptographic information includes

bit pattern information/(S) showing a certain bit sequence, and the part specifying means detects,

in the content data, bit data that matches the bit sequence/(S) shown in the bit pattern

information/(S), and uses a location of the bit data as a basis for specifying the certain part/data

segment, the certain part having a fixed positional relationship to the bit data (see col. 5, lines 23-37 & col. 6, lines 1-5).

Regarding claim 44, Yorke-Smith discloses that the cryptographic information/control block includes a reference instruction/(S and L_2) indicating that the data section/segment in the content data be referred to (see col. 5, lines 23-37), the data section showing a length/L_2 of the certain part/data segment (see col. 4, lines 46-54), and the part specifying means specifies the certain part by referring to the data section/segment as indicated by the reference instruction/(S and L_2) (see col. 5, lines 23-37 & col. 9, lines 15-26) and calculating the length/L_1 (see col. 4, lines 46-54) of the certain part based on the referenced data section (see col. 4, lines 23-54 & col. 5, lines 23-37).

Regarding claim 47, Yorke-Smith discloses the cryptographic information/control block further including at least one piece of algorithm information/F for specifying an algorithm/encryption function used for cryptographic processing (see col. 3, lines 49-50), and the cryptographic processing means/encryption means performing one of encryption and decryption on the certain part/data segment using the specified algorithm/encryption function (see Fig. 6 & col. 2, lines 50-64).

Regarding claim 48, Yorke-Smith discloses the cryptographic information including a plurality of pieces of algorithm/encryption function information (see col. 2, lines 65-67 & col. 3, lines 1-2), and pieces of range information/(L_1, L_2, S) each showing a range over which an algorithm is applied (see col. 4, lines 41-45), and the cryptographic processing means selecting, for each application range in the certain part/data segment, a piece of the algorithm information/encryption function based on the range information/(L_1, L_2, S), and using an

algorithm/encryption function specified by the piece of algorithm information to perform one of

the encryption and decryption on the application range (see col. 2, lines 50-67, col. 3, lines 1-9 &

col. 4, lines 23-54).

Regarding claim 66, the method claim is substantially equivalent to apparatus claim 42.

Therefore, claim 66 is rejected under similar rationale.

Regarding claim 67, the method claim is substantially equivalent to apparatus claim 43.

Therefore, claim 67 is rejected under similar rationale.

Regarding claim 68, the method claim is substantially equivalent to apparatus claim 44.

Therefore, claim 68 is rejected under similar rationale.

Regarding claim 69, the method claim is substantially equivalent to apparatus claim 47.

Therefore, claim 69 is rejected under similar rationale.

Regarding claim 84, method claim is substantially equivalent to apparatus claim 42.

Therefore, claim 84 is rejected under similar rationale.

Claim Rejections - 35 USC § 103

7.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8.   Claims 1-5, 8-14, 16, 17, 70-76, 78 & 79 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Yorke-Smith in view of U.S. Patent 6,052,780 to Glover.

Regarding claim 1, Yorke-Smith discloses reading content data/data segments (see col. 1,
lines 48-60) and cryptographic information/control block from a storage medium/disc drive (see
col. 5, lines 23-37 & col. 6, lines 1-5), the cryptographic information including information/(S
and L_2) used to specify a certain part of the content data on which cryptographic processing is to
be performed (see col. 5, lines 27-37), a part specifying means for specifying, based on the read
cryptographic information, the certain part of the read content data (see col. 5, lines 23-37 & col.
6, lines 1-5), and a cryptographic processing means/encryption means for performing one of
encryption or decryption on the certain part of the read content data (see col. 5, lines 23-37 &
col. 6, lines 1-5). Yorke-Smith lacks the storage medium being portable. However, Glover
teaches that encrypting multimedia content and distributing the content on portable media, such
as DVD or CD-ROM prevents unauthorized copying of the content (see col. 3, lines 1-18 & 36-
50). Therefore, it would have been obvious to one having ordinary skill in the art at the time the
invention was made to use a portable medium in the Yorke-Smith system. One of ordinary skill
in the art would have been motivated to perform such a modification to store data, as a means to
securely distribute multimedia data, as taught by Glover (see col. 3, lines 1-18 & 36-50).

Regarding claim 2, Yorke-Smith, as modified above, discloses a plurality of pieces of
content data are recorded as a file on the storage medium (see col. 6, lines 1-5), along with the
cryptographic information/control block for each of a plurality of file types (see col. 5, lines23-
37 & col. 6, lines 1-15), and the data reading means reads, from the storage medium, the content
data/data segments of a file and the cryptographic information/control block for a corresponding
file type (see col. 1, lines 48-60 & col. 6, lines 1-15).

Regarding claims 3 & 10, as modified above, Yorke-Smith discloses that the cryptographic information/control block includes a reference instruction/(S and L_2) indicating that the data section/segment in the content data be referred to (see col. 5, lines 23-37), and the part specifying means specifies the certain part by referring to the data section/segment as indicated by the reference instruction/(S and L_2) (see col. 5, lines 23-37 & col. 9, lines 15-26).

Regarding claim 4, as modified above, Yorke-Smith discloses that the cryptographic information includes bit pattern information/(S) showing a certain bit sequence, and the part specifying means detects, in the content data, bit data that matches the bit sequence/(S) shown in the bit pattern information/(S), and uses a location of the bit data as a basis for specifying the certain part/data segment, the certain part having a fixed positional relationship to the bit data (see col. 5, lines 23-37 & col. 6, lines 1-5).

Regarding claim 5, as modified above, Yorke-Smith discloses that the indicated data section shows a length/L_2 of the certain part/data segment (see col. 4, lines 46-54), and the part specifying means specifies the certain part of the content data/data segment by referring to the data section as indicated by the reference instruction/(S and L_2), and calculating the length/L_1 (see col. 4, lines 46-54) of the certain part based on the referenced data section (see col. 4, lines 23-54 & col. 5, lines 23-37).

Regarding claim 8, 9 & 13, as modified above, Yorke-Smith discloses the cryptographic information/control block further including at least one piece of algorithm information/F for specifying an algorithm/encryption function used for cryptographic processing (see col. 3, lines 49-50), and the cryptographic processing means/encryption means performing one of encryption

and decryption on the certain part/data segment using the specified algorithm/encryption

function (see Fig. 6 & col. 2, lines 50-64).

Regarding claims 11 & 16, as modified above, Yorke-Smith discloses the cryptographic

processing means encrypting the certain part (see Fig. 4), and the cryptographic apparatus further

comprising a content data recording means/output means (see Fig. 7) for recording the encrypted

content data onto the storage medium/disk drive (see Fig. 7).

Regarding claim 12 & 17, as modified above, Yorke-Smith discloses the cryptographic

processing means decrypting the certain part of the content data (see Fig. 6 & col. 5, lines 27-

37), and the cryptographic apparatus further comprising an encrypting information reading

means/input means for reading, from another portable storage medium/disc drive encrypting

information including information used to specify a certain part in the decrypted content data to

be encrypted (see Fig. 6 & Fig. 7).

Regarding claim 14, as modified above, Yorke-Smith discloses the cryptographic

information including a plurality of pieces of algorithm/encryption function information (see col.

2, lines 65-67 & col. 3, lines 1-2), and pieces of range information/(L_1, L_2, S) each showing a

range over which an algorithm is applied (see col. 4, lines 41-45), and the cryptographic

processing means selecting, for each application range in the certain part/data segment, a piece of

the algorithm information/encryption function based on the range information/(L_1, L_2, S), and

using an algorithm/encryption function specified by the piece of algorithm information to

perform one of the encryption and decryption on the application range (see col. 2, lines 50-67,

col. 3, lines 1-9 & col. 4, lines 23-54).

Regarding claim 70, Yorke-Smith discloses a content data recording area/disc drive (see

Fig. 7) in which content data, of which a certain part has been encrypted, is recorded (see col. 2,

lines50-64), and a cryptographic information recording area/control block in which

cryptographic information, including information used to specify the certain part of the content

data/data segment, is recorded (see Fig. 4, col. 2, lines 50-64, col. 4, lines 55-67 & col. 5, lines 1-

26). Yorke-Smith lacks a *portable* storage medium. However, Glover teaches that encrypting

multimedia content and distributing the content on portable media, such as DVD or CD-ROM

prevents unauthorized copying of the content (see col. 3, lines 1-18 & 36-50). Therefore, it

would have been obvious to one having ordinary skill in the art at the time the invention was

made to use a portable medium in the Yorke-Smith system. One of ordinary skill in the art

would have been motivated to perform such a modification to store data, as a means to securely

distribute multimedia data, as taught by Glover (see col. 3, lines 1-18 & 36-50).

Regarding claim 71, Yorke-Smith, as modified above, discloses each of a plurality of

pieces of encrypted content data being recorded as a file in the content data recording area (see

col. 5, lines 11-37 & col. 6, lines 1-15), and cryptographic information is recorded in the

cryptographic information recording area according to file type/format (see col. 5, lines 11-22).

Regarding claim 72, as modified above, Yorke-Smith discloses the cryptographic

information/control block (see col. 5, lines 23-37), but lacks a reference instruction instructing a

decrypting apparatus decrypting the content data to refer to a data section in the content data.

However, Glover teaches that a self-decrypting digital information product, including

instructions for decryption, allows easy distribution and prevents unauthorized copying (see col.

3, lines 1-18 & 36-50 & col. 4, lines 36-64). Therefore, it would have been obvious to one

having ordinary skill in the art at the time the invention was made to include a reference

instruction for instructing a decryption apparatus to refer to a data section in the content data to

perform decryption on the content. One of ordinary skill in the art would have been motivated to

perform such a modification to allow easy distribution and to prevent unauthorized copying, as

taught by Glover (see col. 3, lines 1-18 & 36-50 & col. 4, lines 36-64).

Regarding claim 73, Yorke-Smith, as modified above, discloses that the cryptographic

information includes bit pattern information/(S) showing a certain bit sequence, and the certain

part having a fixed positional relationship to the bit data (see col. 5, lines 23-37 & col. 6, lines 1-

5). Yorke-Smith lacks an instruction instructing the decrypting apparatus to detect, in the

content data, bit data matching the certain bit sequence/(S) and use a location of the bit data as a

basis for specifying the certain part. However, Glover teaches that a self-decrypting digital

information product, including instructions for decryption, allows easy distribution and prevents

unauthorized copying (see col. 3, lines 1-18 & 36-50 & col. 4, lines 36-64). Therefore, it would

have been obvious to one having ordinary skill in the art at the time the invention was made to

include instructions for instructing a decryption apparatus to detect matching bit data in the

content data. One of ordinary skill in the art would have been motivated to perform such a

modification to allow easy distribution and to prevent unauthorized copying, as taught by Glover

(see col. 3, lines 1-18 & 36-50 & col. 4, lines 36-64).

Regarding claim 74, Yorke-Smith, as modified above, discloses that the indicated data

section shows a length/L_2 of the certain part/data segment (see col. 4, lines 46-54), and the part

specifying step specifies the certain part of the content data/data segment by referring to the data

section as indicated by the reference instruction/(S and L_2), and calculating the length/L_1 (see

col. 4, lines 46-54) of the certain part based on the referenced data section (see col. 4, lines 23-54

& col. 5, lines 23-37).

Regarding claims 75 & 78, as modified above, Yorke-Smith discloses at least one piece

of algorithm information/F for specifying an algorithm/encryption function to be used when

decrypting the content data (see col. 3, lines 49-50).

Regarding claim 76, Yorke-Smith, as modified above, discloses the cryptographic

information/control block including a reference instruction/(S and L_2) indicating that the data

section/segment in the content data be referred to (see col. 5, lines 23-37).

Regarding claim 79, Yorke-Smith, as modified above, discloses the cryptographic

information including a plurality of pieces of algorithm/encryption function information (see col.

2, lines 65-67 & col. 3, lines 1-2), and pieces of range information/(L_1, L_2, S) each showing a

range over which an algorithm is applied (see col. 4, lines 41-45).

9.   Claims 18, 58, 59 & 82 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Yorke-Smith in view of Glover, as applied to claim 17, in further view of U.S. Patent 5,475,757

to Kelly.

Regarding claim 18, Yorke-Smith discloses an encrypting information reading

means/input means for reading, from another portable storage medium/disc drive (see Fig. 7),

encrypting information/control block including information used to specify a certain part/data

segment in the content data to be decrypted (see col. 4, lines 23-54, col. 5, lines 23-37 & col. 6,

lines 1-5) and a content data recording means/output means (see Fig. 7) for recording the

encrypted content data onto the other storage medium. Yorke-Smith lacks encrypting data based

on the control blocks of decrypted data. However, Kelly teaches that when an intermediary is involved in a transmission, a message is decrypted, and then re-encrypted using the same algorithm and secret code key to safeguard the message (see col. 10, lines 23-48). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to specify a certain part/data segment to be encrypted in decrypted content data according to encrypting information and to encrypt the part specified by the encrypting information. One of ordinary skill in the art would have been motivated to perform such a modification to safeguard a message as it is transmitted through and intermediary through and intermediary, as taught by Kelly (see col. 10, lines 23-48).

Regarding claim 58, the method claim is substantially equivalent to apparatus claim 18. Therefore, claim 58 is rejected under similar rationale.

Regarding claim 59, Yorke-Smith discloses the storage medium/disc drive storing a plurality of pieces of content data/data segments as files, along with cryptographic information/control blocks for a plurality of file types corresponding to files that can be stored on the storage medium (see col. 5, lines 23-26), and the cryptographic information reading means/input means reads the cryptographic information/control block (see Fig. 4) for a file type/format (see col. 5, lines 11-22) from the storage medium, and the content data recording means/output means records the encrypted content data onto the storage medium/disc drive as a file of the file type/format (see col. 5, lines 11-22) corresponding to the read cryptographic information/control block (see col. 4, lines 55-67 & col. 5, lines 1-26).

Regarding claim 82, the method claim is substantially equivalent to apparatus claim 18. Therefore, claim 82 is rejected under similar rationale.

10.   Claims 19-27, 51-57, 60, 61 & 81 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Yorke-Smith in view of Glover, in further view of Kelly.

Regarding claim 19, Yorke-Smith discloses a content data obtaining means/input means

for obtaining content data (see Fig. 7), a cryptographic information reading means/input means

for reading, from portable storage medium/disc drive (see Fig. 7), cryptographic

information/control block including information used to specify a certain part of the content

data/data segment on which cryptographic processing/decryption is to be performed (see col. 2,

lines 65-67 & col. 3, lines 1-9), a part specifying means for specifying the certain part of the

obtained content data based on the read cryptographic information (see col. 3, lines 1-9 & col. 4,

lines 23-54), a cryptographic processing means for encrypting a certain part (see col. 2, lines 50-

64), and a content data recording means/output means (see Fig. 7) for recording the encrypted

content data onto the storage medium/disc drive (see Fig. 7). Yorke-Smith discloses generating

the cryptographic information/control block, writing to the storage medium/disc drive and

reading the cryptographic information/control block for decryption purposes, but lacks

encryption based on the cryptographic information/control block. However, Kelly teaches that

when an intermediary is involved in a transmission, a message is decrypted, and then re-

encrypted using the same algorithm and secret code key to safeguard the message (see col. 10,

lines 23-48). Therefore, it would have been obvious to one having ordinary skill in the art at the

time the invention was made to specify a certain part/data segment to be encrypted in the control

block and to include means to encrypt the part specified by the cryptographic information. One

of ordinary skill in the art would have been motivated to perform such a modification to

safeguard a message as it is transmitted through and intermediary, as taught by Kelly (see col. 10, lines 23-48).

Regarding claim 20, Yorke-Smith, as modified above, discloses the storage medium/disc drive storing a plurality of pieces of content data/data segments as files, along with cryptographic information/control blocks for a plurality of file types corresponding to files that can be stored on the storage medium (see col. 5, lines 23-26), and the cryptographic information reading means/input means reads the cryptographic information/control block (see Fig. 4) for a file type/format (see col. 5, lines 11-22) from the storage medium, and the content data recording means/output means records the encrypted content data onto the storage medium/disc drive as a file of the file type/format (see col. 5, lines 11-22) corresponding to the read cryptographic information/control block (see col. 4, lines 55-67 & col. 5, lines 1-26).

Regarding claim 21, Yorke-Smith, as modified above, discloses that the cryptographic information includes bit pattern information/(S) showing a certain bit sequence, and the part specifying means detects, in the content data, bit data that matches the bit sequence/(S) shown in the bit pattern information/(S), and uses a location of the bit data as a basis for specifying the certain part/data segment, the certain part having a fixed positional relationship to the bit data (see col. 5, lines 23-37 & col. 6, lines 1-5).

Regarding claims 22 & 25, Yorke-Smith, as modified above, discloses that the cryptographic information/control block includes a reference instruction/(S and L_2) indicating that the data section/segment in the content data be referred to (see col. 5, lines 23-37), the data section showing a length/L_2 of the certain part/data segment (see col. 4, lines 46-54), and the part specifying means specifies the certain part by referring to the data section/segment as indicated

by the reference instruction/(S and L_2) (see col. 5, lines 23-37 & col. 9, lines 15-26) and

calculating the length/L_1 (see col. 4, lines 46-54) of the certain part based on the referenced data

section (see col. 4, lines 23-54 & col. 5, lines 23-37).

Regarding claim 23 & 26, Yorke-Smith, as modified above, discloses the cryptographic

information/control block further including at least one piece of algorithm information/F for

specifying an algorithm/encryption function used for cryptographic processing (see col. 3, lines

49-50), and the cryptographic processing means/encryption means performing one of encryption

and decryption on the certain part/data segment using the specified algorithm/encryption

function (see Fig. 6 & col. 2, lines 50-64).

Regarding claim 24, Yorke-Smith discloses that the cryptographic information includes

bit pattern information/(S) showing a certain bit sequence, and the part specifying means detects,

in the content data, bit data that matches the bit sequence/(S) shown in the bit pattern

information/(S), and uses a location of the bit data as a basis for specifying the certain part/data

segment, the certain part having a fixed positional relationship to the bit data (see col. 5, lines 23-

37 & col. 6, lines 1-5).

Regarding claim 27, Yorke-Smith discloses the cryptographic information including a

plurality of pieces of algorithm/encryption function information (see col. 2, lines 65-67 & col. 3,

lines 1-2), and pieces of range information/(L_1, L_2, S) each showing a range over which an

algorithm is applied (see col. 4, lines 41-45), and the cryptographic processing means selecting,

for each application range in the certain part/data segment, a piece of the algorithm

information/encryption function based on the range information/(L_1, L_2, S), and using an

algorithm/encryption function specified by the piece of algorithm information to perform one of

the encryption and decryption on the application range (see col. 2, lines 50-67, col. 3, lines 1-9 & col. 4, lines 23-54).

Regarding claim 51, the method claim is substantially equivalent to apparatus claim 1. Therefore, claim 51 is rejected under similar rationale.

Regarding claim 52, the method claim is substantially equivalent to apparatus claim 2. Therefore, claim 52 is rejected under similar rationale.

Regarding claim 53, the method claim is substantially equivalent to apparatus claim 4. Therefore, claim 53 is rejected under similar rationale.

Regarding claim 54, the method claim is substantially equivalent to apparatus claim 8. Therefore, claim 54 is rejected under similar rationale.

Regarding claim 55, the method claim is substantially equivalent to apparatus claim 11. Therefore, claim 55 is rejected under similar rationale.

Regarding claim 56, the method claim is substantially equivalent to apparatus claim 17. Therefore, claim 56 is rejected under similar rationale.

Regarding claim 57, the method claim is substantially equivalent to apparatus claim 12. Therefore, claim 57 is rejected under similar rationale.

Regarding claim 60, the method claim is substantially equivalent to apparatus claim 4. Therefore, claim 60 is rejected under similar rationale.

Regarding claim 61, the method claim is substantially equivalent to apparatus claim 8. Therefore, claim 61 is rejected under similar rationale.

Regarding claim 81, the method claim is substantially equivalent to apparatus claim 1. Therefore, claim 81 is rejected under similar rationale.

11.   Claims 29-31, 34, 37-39, 41, 50, 62, 63, 65 & 83 are rejected under 35 U.S.C. 103(a) as

being unpatentable over Yorke-Smith in view of U.S. Patent 5,875,349 to Cornaby et al.

(Cornaby).

Regarding claim 29, Yorke-Smith discloses a data obtaining means/input means for

obtaining, from received data, content data (see Fig. 7), and cryptographic information/control

block including information used to specify a certain part of the content data/data segment on

which cryptographic processing/decryption is to be performed (see col. 2, lines 65-67 & col. 3,

lines 1-9), the received data consisting of content data and cryptographic information/control

block that been transmitted from a storage medium, such as a disc drive (see Fig. 7), a part

specifying means for specifying the certain part of the obtained content data based on the

obtained cryptographic information/control block (see col. 3, lines 1-9 & col. 4, lines 23-54), and

a cryptographic processing means/encryption means for performing one of encryption and

decryption on the certain part of the content data (see Fig. 6 & Fig. 7). Yorke-Smith does not

disclose the transmitted information being multiplexed. However, Cornaby teaches an

arrangement for allowing a computer to communicate with a storage device, over a bus, such as a

multiplexed bus (see col. 11, lines 64-67 & col. 12, lines 1-16), that allows the computer to

control some of the operations of the storage device, reducing the cost and complexity of the

drive (see col. 9, lines 23-36). Therefore, it would have been obvious to one having ordinary

skill in the art at the time the invention was made to use the Cornaby arrangement, with a

multiplexed bus, in the Yorke-Smith system. One of ordinary skill in the art would have been

motivated to perform such a modification to gain the benefit of reduced cost and complexity in

the storage device, as taught by Cornaby (see col. 9, lines 23-36, col. 11, lines 64-67 & col. 12,

lines 1-16).

Regarding claim 30, Yorke-Smith discloses that the cryptographic information/control

block includes a reference instruction/(S and L_2) indicating that the data section/segment in the

content data be referred to (see col. 5, lines 23-37), and the part specifying means specifies the

certain part by referring to the data section/segment as indicated by the reference instruction/(S

and L_2) (see col. 5, lines 23-37 & col. 9, lines 15-26).

Regarding claim 31, Yorke-Smith discloses that the cryptographic information/control

block includes sync pattern information/(S) showing a certain bit sequence, and the part

specifying means detects, in the content data, a sync pattern data that matches the bit

sequence/(S) shown in the bit pattern information/(S), and uses a location of the bit data as a

basis for specifying the certain part/data segment, the certain part having a fixed positional

relationship to the bit data (see col. 5, lines 23-37 & col. 6, lines 1-5).

Regarding claim 34, Yorke-Smith discloses that the indicated data section shows a

length/L_2 of the certain part/data segment (see col. 4, lines 46-54), and the part specifying means

specifies the certain part of the content data/data segment by referring to the data section as

indicated by the reference instruction/(S and L_2), and calculating the length/L_1 (see col. 4, lines

46-54) of the certain part based on the referenced data section (see col. 4, lines 23-54 & col. 5,

lines 23-37).

Regarding claims 37 & 38, as best understood, Yorke-Smith discloses the cryptographic

information/control block further including at least one piece of algorithm information/F for

specifying an algorithm/encryption function used for cryptographic processing (see col. 3, lines

49-50), and the cryptographic processing means/encryption means performing one of encryption

and decryption on the certain part/data segment using the specified algorithm/encryption

function (see Fig. 6 & col. 2, lines 50-64).

Regarding claim 39, Yorke-Smith discloses the cryptographic information including a

plurality of pieces of algorithm/encryption function information (see col. 2, lines 65-67 & col. 3,

lines 1-2), and pieces of range information/(L_1, L_2, S) each showing a range over which an

algorithm is applied (see col. 4, lines 41-45), and the cryptographic processing means selecting,

for each application range in the certain part/data segment, a piece of the algorithm

information/encryption function based on the range information/(L_1, L_2, S), and using an

algorithm/encryption function specified by the piece of algorithm information to perform one of

the encryption and decryption on the application range (see col. 2, lines 50-67, col. 3, lines 1-9 &

col. 4, lines 23-54).

Regarding claim 41, Yorke-Smith discloses the cryptographic processing means

decrypting the certain part/data segment (see Fig. 6).

Regarding claim 50, Yorke-Smith discloses the cryptographic processing means

encrypting the certain part of the content data (see col. 2, lines 50-64) but lacks multiplexing.

However, Cornaby teaches an arrangement for allowing a computer to communicate with a

storage device, over a bus, such as a multiplexed bus (see col. 11, lines 64-67 & col. 12, lines 1-

16), that allows the computer to control some of the operations of the storage device, reducing

the cost and complexity of the drive (see col. 9, lines 23-36). Therefore, it would have been

obvious to one having ordinary skill in the art at the time the invention was made to use the

Cornaby arrangement, with a multiplexed bus, in the Yorke-Smith system to multiplex and

transmit the multiplex data. One of ordinary skill in the art would have been motivated to

perform such a modification to gain the benefit of reduced cost and complexity in the storage

device, as taught by Cornaby (see col. 9, lines 23-36, col. 11, lines 64-67 & col. 12, lines 1-16).

Regarding claim 62, the method claim is substantially equivalent to apparatus claim 29.

Therefore, claim 62 is rejected under similar rationale.

Regarding claim 63, the method claim is substantially equivalent to apparatus claim 31.

Therefore, claim 63 is rejected under similar rationale.

Regarding claim 65, the method claim is substantially equivalent to apparatus claim 37.

Therefore, claim 65 is rejected under similar rationale.

Regarding claim 83, method claim is substantially equivalent to apparatus claim 29.

Therefore, claim 83 is rejected under similar rationale.

Allowable Subject Matter

12.   Claims 6, 15, 28, 32, 35, 40, 45, 49, 64 & 80 are objected to as being dependent upon a

rejected base claim, but would be allowable if rewritten in independent form including all of the

limitations of the base claim and any intervening claims.

13.   The following is a statement of reasons for the indication of allowable subject matter:

d.   Regarding claims 15, 28, 40, 49 & 80, the prior art relied upon fails to teach or

suggest cryptographic information including priority ratings indicating an order in which

the pieces of algorithm information should be applied.

e.   Regarding claims 6, 35 & 45, the prior art relied upon fails to teach or suggest the

cryptographic information including a value showing a unit used for the indicated data

section, and specifying the certain part by multiplying the length shown by the data

section with the unit value to calculate the length of the certain part.

f.   Regarding claims 32 & 64, the prior art relied upon fails to teach or suggest

verifying the authenticity of the detected sync pattern by checking whether another sync

pattern is located at a position a set interval away from the location of the detected sync

pattern.

Conclusion

14.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

a.   U.S. Patents 6,490,353 & 5,261,003 were cited for relevance in using multiple

encryption algorithms on blocks of data.

b.   U.S. Patent 6,314,409 was cited for relevance in encrypted multimedia

distribution techniques involving more than one encryption algorithm.

c.   U.S. Patent 6,550,009 was cited for relevance in using portable media to distribute

encrypted data.

d.   "The Effect of Algorithm-Agile Encryption on ATM Quality of Service" was

cited for issues and motivations surrounding using multiple encryption algorithms.

15.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191.

The examiner can normally be reached on Monday - Thursday, 8:00 a.m. - 5:30 p.m.. The

examiner can also be reached on alternate Fridays from 8:00 a.m. – 4:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED"
or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive,
Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should
be directed to the receptionist whose telephone number is (703) 305-9000.

NORMAN M. WRIGHT
PRIMARY EXAMINER

MJS
28 January 2004